Statement of Laura H. Parsky
Deputy Assistant Attorney General
Criminal Division, U.S. Department of Justice
Before the U.S. House of Representatives, Committee on the Judiciary,
Subcommittee on Crime, Terrorism and Homeland Security

REAUTHORIZATION OF THE USA PATRIOT ACT TECHNOLOGY PROVISIONS

April 21, 2005

I. Introduction

Good morning, Mr. Chairman, Ranking Member Scott, and Honorable Members of the Subcommittee. It is my pleasure to appear before you to discuss some of the provisions of the PATRIOT Act that have modernized our laws to address new technologies.

In particular, you have invited me to discuss sections 209, 217, and 220 of the Act. Section 209 rendered the rules for stored voicemail messages more consistent with those for other types of stored messages such as electronic mail (e-mail) and answering machine messages. Prior to the Act, access to stored voicemails was unnecessarily encumbered by rules designed to apply to on-going access to live communications rather than the rules for a single access to stored communications. Section 217 recognized the growth of computer networks and makes clear that federal law will not shield a person who trespasses on the computer system of another. Section 217 put the power to

decide who may enter property back where it belongs, in the hands of the property owner, just as has been the case for real property owners throughout history. Finally, Section 220 recognized that today's modern communications technologies make it possible for records relating to an investigation to be dispersed across the country. Section 220 allowed the prosecutor and investigator most familiar with the case to prepare the affidavits and applications to seek a search warrant, while the judge most familiar with the investigation may authorize the warrant for related records.

In the three and a half years since Congress passed these provisions of the PATRIOT Act by overwhelming bipartisan majorities, we have had the opportunity to carefully assess the true utility of these new tools. I am here to report to you that we in law enforcement have found these tools critical to our mission to protect national security and the safety of our communities. As I will discuss further in a moment, we have used tools created in the PATRIOT Act to disrupt terrorist networks and to prevent terrorist attacks, to bring violent fugitives to justice, and to rescue children in imminent danger. The PATRIOT Act has allowed law enforcement to be more effective and more efficient. All this has been done without sacrificing any of the constitutional protections or invaluable privacy rights that we as Americans hold dear.

Members of the Subcommittee, we cannot go back. If Congress fails to re-authorize sections 209, 217 and 220 of the PATRIOT Act, we will revert to old rules that fail to account for today's technological innovations, that treat similar situations differently, and that create inefficient processes and unnecessary delay. The tools contained in the PATRIOT Act have been essential to the Department's top priorities, chief of which is to ensure public safety against threats both foreign and domestic. If these provisions are not renewed, the Department's ability to combat not only terrorism but also other serious offenses such as cybercrime, child pornography, and kidnapings will be less efficient and less effective. There are carefully adhered to limits on these authorities, and experience has proven their utility and rationality. In light of the very real threats we face today, we cannot afford to return to a time when technology was outpacing the tools of law enforcement. Therefore, I am here to ask that you preserve these critical tools in today's world of advancing technology and re-authorize these provisions of the PATRIOT Act.

II. Section 209 Harmonized the Treatment of Stored Voicemail Messages With That of Other Types of Stored Messages.

Section 209 provides a good example of how the PATRIOT Act modernized the law to recognize new technology. Prior to the Act, voicemail --

essentially a remote answering machine service -- was treated differently than other remote storage services, like e-mail, or even than more traditional answering machine messages. Answering machine messages can be obtained with an ordinary search warrant issued by a judge upon a showing of probable cause. Likewise, e-mail messages can be obtained with a search warrant. By contrast, however, voicemail messages were subject to the much more burdensome and restrictive process of obtaining a wiretap order.

The Wiretap Act (18 U.S.C. 2510 *et seq.*) was designed to address a very particular type of situation, the ongoing interception of real-time conversations. Given the power of this law enforcement technique, it is properly subject to strict limitations. However, the one-time access to stored communications, such as a voicemail message, does not implicate the same sensitivities associated with the ongoing interception of live telephonic communications; therefore, there is no basis for subjecting requests to retrieve voicemail messages to the same special protections as requests for wiretaps. This is especially true when law enforcement could obtain the same type of information with a search warrant had the information been stored on an answering machine in a person's home instead of with a third-party provider. Even where the additional requirements of the Wiretap Act could be met, law enforcement was forced to waste precious

time and resources to satisfy these more burdensome requirements.

Section 209 of the PATRIOT Act made existing statutes technology-neutral by providing that access to voicemail messages not be subjected to a higher standard than access to e-mail or answering machine messages. Now investigators can go to a judge and obtain a search warrant to access voicemail messages stored by a third-party provider. Yet, section 209 preserved all of the checks and balances inherent in the process for accessing other stored communications, including ensuring that neutral judges evaluate such applications for probable cause when a search warrant is sought. Further, by applying the same rules to voicemail messages as to other stored communications, section 209 eliminated needlessly burdensome and anachronistic rules that threatened the ability of law enforcement to successfully and effectively investigate and prosecute serious crimes.

Since the passage of the PATRIOT Act, search warrants have been used in a variety of criminal cases to obtain voicemails that provided critical evidence. Investigators have obtained voicemail messages left for both foreign and domestic terrorists. In addition, warrants made possible by the Act have been used to investigate a large-scale international ecstasy smuggling ring. In another case, investigators were able to quickly obtain a warrant to retrieve the

voicemails of a defendant arrested in possession of hundreds of pounds of marijuana worth over half a million dollars on the street.

Allowing section 209 to expire, as will happen at the end of this year if Congress fails to act, would take us back to the irrationality of applying different rules for access to similar types of stored messages. Going back to requiring a wiretap order for access to stored voicemail messages would needlessly hamper law enforcement efforts to investigate crimes and obtain evidence in a timely manner. We need not and should not go back to this inconsistent, ineffective, and inefficient process.

III. Section 217 Gave Modern Computer Owners the Same Rights That Homeowners Have Always Had -- Ultimate Control Over Who May Enter Their Property.

Section 217 of the PATRIOT Act (the Hacker Trespass Provision) also brought criminal procedures up to date with modern technology. Homeowners have always had the right to decide who can and who cannot enter their property, including the right to decide whether or not to invite law enforcement onto their property to investigate a crime. Where someone breaks and enters into a home, the law does not protect the thief from police officers when the homeowner has invited in the police to catch the trespasser.

One would not expect that someone who breaks and enters into a

computer system would have any more right to be shielded from law enforcement than a common trespasser. The law certainly should not protect the purported privacy of a trespasser at the very same time he is violating the privacy of the computer owner, potentially accessing sensitive information ranging from trade secrets to medical information to personal letters.

Prior to the passage of the Hacker Trespass Provision, the law did not clearly provide that a computer owner could invite the assistance of law enforcement in monitoring computer hackers on his or her system. In what one legal commentator called a "bizarre result,"[1] it was possible for the intruder invading the privacy of a computer owner to himself claim that his invasion should be kept private from investigators.

The Hacker Trespass Provision left no doubt that a computer owner has the authority to control who is on his or her system. That right includes the ability to invite law enforcement to help combat hackers and other cyber-intruders. In keeping with the principle of preserving the computer owner's rights, the Hacker Trespass Provision did not *require* computer owners to involve law enforcement if they detect trespassers on their systems; it simply gave them the *option* to do so.

---

[1] Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 Wash. & Lee L. Rev. 1287, 1300 (2000).

On the other hand, someone with no right to be on that system cannot be heard to complain when law enforcement uncovers his unauthorized activities.

In fact, the Hacker Trespass Provision did not adversely affect any legitimate privacy rights. Prior to the passage of the PATRIOT Act, the Wiretap Act already allowed computer owners to monitor activity on their machines to protect their rights and property. Thus, trespassers' communications were already subject to monitoring; it was simply unclear whether computer owners could obtain the assistance of law enforcement to conduct such monitoring. Because computer owners often lack the expertise, equipment, or financial resources required to monitor their systems themselves, they commonly have no effective way to exercise their rights to protect themselves from unauthorized attackers. The Hacker Trespass Provision ensured that computer owners could effectively protect their rights through the assistance of law enforcement.

The Hacker Trespass Provision also preserved the privacy of law-abiding computer users by sharply limiting the circumstances under which the provision applies. Law enforcement may only monitor a computer when invited to do so by the computer owner, and even then they may not agree to assist unless (1) they are engaged in a lawful investigation; (2) there is reason to believe that the communications will be relevant to that investigation; and (3) their activities will

not acquire any communications beyond those authorized. Moreover, the Hacker Trespass Provision provided a narrow definition of "computer trespasser," which excludes individuals who have a contractual relationship with the service provider. Therefore, for example, the Hacker Trespass Provision would not allow an Internet Service Provider to ask law enforcement to help monitor a hacking attack on its system that was initiated by one of its own subscribers. Nor can this provision be used if the configuration of the computer system would require the interception of non-consenting authorized users. Of course, the authority to intercept ceases at the conclusion of the investigation or when consent is withdrawn.

Since its enactment, the Hacker Trespass Provision has played a key role in sensitive national security matters, including investigations into hackers' attempts to compromise military computer systems. The Hacker Trespass Provision is also particularly helpful when computer hackers launch massive "denial of service" attacks that are designed to shut down web sites, computer networks, or even the entire Internet.

If Congress were to fail to act before the end of this year to preserve the Hacker Trespass Provision, we would revert to a law that protects criminal rights over victim rights. A computer hacker would be able to compromise the

legitimate privacy rights of his victims, and those victims would be denied law enforcement assistance in catching the perpetrator. As computer hacking becomes more widespread and the threat of cyber-terrorism grows, we simply cannot afford to take a step backward in our efforts to protect victims and to deter this serious crime.

IV. Section 220 Allowed Law Enforcement To Keep Pace With the Modern Reality of Remote Storage of On-line Communications.

Section 220 acknowledged the realities of our modern on-line world, where evidence can be stored anywhere in the country, and section 220 removed the barriers that had stood in the way of law enforcement's ability to respond quickly within those realities. Specifically, section 220 allowed courts with jurisdiction over an investigation to issue search warrants for electronic evidence stored outside of their own district.

Prior to the PATRIOT Act, some courts declined to issue search warrants for e-mail messages stored on servers in other districts. As a result, many time-sensitive investigations were delayed as new investigators, prosecutors, and judges in other districts with no prior familiarity with the investigation were brought up to speed. Moreover, requiring investigators to obtain warrants in the jurisdiction where an Internet Service Provider happened to locate its servers

placed enormous burdens on a few districts where major Internet Service Providers are located, such as the Northern District of California and the Eastern District of Virginia.

Section 220 provided a rational solution to these problems. Now, investigators have one place to go to seek a search warrant for electronic evidence, the district where the investigation is being conducted, rather than having to duplicate their efforts in other districts just because electronic records happen to be stored there. For instance, section 220 would allow a judge with jurisdiction over a murder investigation in Pennsylvania to issue a search warrant for e-mail messages pertaining to that investigation that happen to be stored on a server in Silicon Valley, California. Under this scenario, the judge in Pennsylvania most familiar with the investigation could issue the warrant, rather than a judge in the Northern District of California, who is completely unfamiliar with the case.

The Department of Justice has already utilized section 220 in extremely important terrorism investigations. As the Criminal Division's Assistant Attorney General, Christopher Wray, testified before the Senate's Committee on the Judiciary on October 21, 2003, section 220 proved useful in the Portland terror cell case, because "the judge who was most familiar with the case was able to

issue the search warrants for the defendants' e-mail accounts from providers in other districts, which dramatically sped up the investigation and reduced all sorts of unnecessary burdens on other prosecutors, agents and courts." This provision of the PATRIOT Act has been similarly useful in the "Virginia Jihad" case involving a Northern Virginia terror cell and in the case of the infamous "shoebomber" terrorist, Richard Reid.

In addition to terrorism cases, section 220 has also been used effectively in a vast array of criminal investigations where perpetrators generated electronic evidence in numerous distant jurisdictions through their on-line activities, whether or not their crimes actually occurred on-line. Take for example the recent case of a man who, armed with a sawed-off shotgun, abducted and sexually assaulted his estranged wife in West Virginia. He later fled West Virginia in a stolen car to avoid capture. While on the run, he continued to contact associates by e-mail using an Internet Service Provider whose e-mail servers happened to be located clear across the country in California. Using the authority provided by section 220, investigators in West Virginia were able to obtain a warrant quickly from a federal court in West Virginia for the disclosure of information regarding the armed fugitive's e-mail account. The Internet Service Provider quickly provided information revealing that the fugitive had logged

onto his e-mail account from South Carolina. Using that information, Deputy U.S. Marshals were able to arrest the fugitive the very next day. He later pleaded guilty in state court and was sentenced to imprisonment for a term of 30 years. The ability to obtain a warrant for e-mail records immediately, made possible by section 220 of the PATRIOT Act, was crucial to capturing this violent fugitive.

Section 220 has also been used to more effectively and more efficiently unravel a complicated international conspiracy to distribute child pornography. Investigators in New Jersey had probable cause to search a number of different computers used by a company that operated its own child pornography websites and provided credit card processing services to other child pornography websites. These computers were physically located in four separate judicial districts; however, a single magistrate in Newark, New Jersey signed search warrants for all four computers. The searches yielded records of tens of thousands of transactions on hundreds of child pornography and erotica websites. The investigation of these criminals exploiting children for profit would have been dramatically handicapped without section 220. With the assistance of the PATRIOT Act, nine individuals or corporations have been convicted of federal crimes. More significantly, the evidence gathered under section 220 has led to nearly a thousand more domestic and foreign arrests.

Section 220 has also dramatically reduced the administrative burdens on judicial districts that are home to large Internet Service Providers. Before the PATRIOT Act, these districts were inundated with search warrant requests for electronic evidence. For example, prior to the passage of the PATRIOT Act, the U.S. Attorney's Office in Alexandria, Virginia was receiving approximately 10 applications each month from United States Attorney's Offices in other districts for search warrants for records from Internet Service Providers. For each of these applications, both an Assistant United States Attorney and a law enforcement agent in the district had to learn all of the facts of another district's investigation in order to apply for the warrant. The result was that agents, attorneys, and judges spent many hours each month processing applications for investigations based in other districts. Thanks to section 220, these attorneys and agents can now spend their time investigating crime in their own districts rather than duplicating the efforts of other districts' investigations and processing unnecessary paperwork.

Contrary to concerns voiced by some, section 220 did not allow investigators to "shop" for sympathetic judges. Section 220 required that the court issuing a search warrant have jurisdiction over the investigation. Investigators may not pick and choose among any court in the country; they

must go to a court with proper jurisdiction. Moreover, nothing in section 220 affected the standard for issuing a search warrant. All of the same requirements apply regardless of whether the warrant is issued where the investigation is being conducted or where the records are located.

In today's world of advanced communications technology, it is imperative that law enforcement have modern tools to keep pace with criminals. Rather than requiring law enforcement to chase down electronic evidence across the country and causing unnecessary delay in time-sensitive investigations, Congress must re-authorize section 220.

V. Many of the Other Provisions of the PATRIOT Act Have Likewise Been Vital To Modernizing 20th Century Laws to Reflect 21st Century Realities.

The provisions I have just discussed are not the only ones in the PATRIOT Act that have modernized our laws and made our rules more consistent with changing technology. To illustrate, I want to touch on just two more of the provisions of the Act that typify the kind of reasonable corrections made by the PATRIOT Act: section 212, the Emergency Disclosure Provision, and section 210, which modernized the terms used to describe information that may be obtained with a subpoena.

Before the PATRIOT Act, an Internet Service Provider was limited in its

ability to voluntarily provide information to the government about an imminent danger, including terrorist plots. Section 212, the Emergency Disclosure Provision, now permits providers voluntarily to disclose subscriber records in life-threatening or other dangerous emergencies. This provision also corrected an anomaly in prior law under which an Internet Service Provider could voluntarily disclose the content of communications to protect itself against hacking, but could not voluntarily disclose stored customer records for the same purpose.

Since its passage, section 212 has repeatedly saved lives. Emergency disclosure has been used to investigate death threats in our schools, to recover victims in kidnaping cases, and to protect targeted government facilities against cyber-attack. But let me describe just one case in particular -- a case where emergency disclosure resulted in the rescue of a 13-year-old girl from her abductor. In early 2002, FBI agents in Pittsburgh received a report from local police that a 13-year-old girl had disappeared the previous day from her parents' home. A friend of the girl told investigators that the girl had discussed leaving home with a man she had met on-line. A few days later, an anonymous caller contacted the FBI and stated that he had chatted on-line recently with an individual claiming to have taken a girl from Pittsburgh. FBI agents in Pittsburgh quickly requested information from an Internet Service Provider

pursuant to section 212. With the information voluntarily provided in response to that request, agents were able to locate the perpetrator at his residence in Herndon, Virginia and rescue the child victim. The girl's abductor was arrested, pleaded guilty to charges including sexual exploitation of a minor, and was sentenced to a prison term of over 19 years.

Although section 210 of the PATRIOT Act is not scheduled to sunset, it provides another good example of how the PATRIOT Act has modernized and updated our laws. In particular, section 210 of the Act clarified the scope of subpoenas for records from electronic communication service providers, such as Internet Service Providers. Section 210 updated old terms that were specific to telephone communications in order to ensure that those terms do not stand in the way of law enforcement's obtaining equivalent types of information associated with modern communications. Thus, for instance, whereas prior law allowed law enforcement to obtain only "local and long distance telephone toll billing records," the PATRIOT Act included parallel terms for communications on computer networks, such as "records of session times and durations." Similarly, the law prior to the PATRIOT Act allowed law enforcement to use a subpoena to obtain the customer's "telephone number or other subscriber number or identity," but did not define what that phrase meant in the context of Internet

communications. Section 210 added "any temporarily assigned network address" to make clear that, among other things, Internet Protocol addresses are included.

These clarifications were put into action in Operation Hamlet, an investigation that dismantled an international ring of child molesters and rescued more than 100 child victims. To give just a few examples, this criminal network used the Internet to exchange photographs and video of their molestation of children, molestation that included children being sexually exploited by their own parents or by different individuals to whom the parents had offered their children for sex. In some instances, molesters would even offer a "live show" of their disgusting acts via a webcam. Subpoenas were issued to numerous Internet Service Providers during the investigation requesting information that was explicitly made subject to subpoena authority by the PATRIOT Act. Among the types of information investigators received were names and addresses, records of when molesters were on-line and for how long, and temporarily assigned network addresses that allowed law enforcement to tie particular customers to their on-line activities. With this information, much of which was unobtainable prior to the PATRIOT Act, investigators were able to identify many of the members of this ring and obtain

search and arrest warrants. Thus far, 26 searches have been conducted in the United States and 11 searches in other countries; and 23 persons have been indicted in the United States, resulting in 21 convictions and two individuals pending trial.

VI. Conclusion

As I have described above, the modern tools Congress authorized through passage of the PATRIOT Act have dramatically improved law enforcement's ability to protect the safety and security of the American people. With these tools, the Department of Justice has captured terrorists, brought violent criminals to justice, and rescued children from sexual exploitation. Most significantly, we have prevented another terrorist attack from striking us here at home. These are facts, not fears. It is in this context that these tools must be weighed. It is this record of accomplishments that should be first and foremost in your minds.

Our world is different today in ways both good and bad. On the one hand, we face the threat of terrorism on a scale that was previously unimaginable. On the other hand, we have experienced tremendous technological advancement that has given us modern wonders like the Internet. It is because of *both* of these developments that the PATRIOT Act is

vital to our nation's safety. We cannot go back to the days before September 11th, and we cannot turn back the clock of the Digital Age; likewise, we cannot regress to outdated laws that defy reason in today's world. Our experience over the past three and a half years clearly demonstrates the real benefits and necessity of the modern law enforcement tools provided in the PATRIOT Act. The Department of Justice appreciates this Subcommittee's leadership in making sure that our country's laws meet the challenges of today and of tomorrow by re-authorizing these provisions of the PATRIOT Act. Thank you for the opportunity to testify today and for your continuing support. I am happy to try to answer any questions you may have.